

SECURE DATA TRANSMISSION VIA MULTICHANNEL
ENTITLEMENT MANAGEMENT AND CONTROL

Field of the Invention

5 **[0001]** This invention relates to the transmission of plural streams of information over separate channels, and more particularly to the spreading of encoding information and transmission of portions thereof by way of separate channels.

Background of the Invention

10 **[0002]** Electronic transmission of information to each of a plurality of users or subscribers of an information providing service is now common, as exemplified by satellite and cable system delivery of television and audio information. FIGURE 1 is a simplified block diagram of a satellite system 10 for delivering information to multiple subscribers or users located over a large area. In FIGURE 1, a ground station 12 with at least an uplink antenna 14 provides streams of information to a receiving or uplink antenna 22 of a spacecraft 20. The spacecraft 20 may be in a geosynchronous orbit, which remains at an apparently fixed location in the sky, as seen from a plurality of users 1, 2, . . . , N. Users 1, 2, . . . , N are located in a coverage area 26 of the beam, illustrated as 25, of a spacecraft transmitting or downlink antenna 24. A ground station, which may be ground station 12 or another ground station, also provides control functions for maintaining the spacecraft 20 in proper orbit and operating condition.

25 **[0003]** The streams of uplink information transmitted by ground station 12 of FIGURE 1 and its antenna 14 to uplink antenna 22 of spacecraft 20 may be somewhat processed in the spacecraft 20, but the spacecraft and its antennas can often be viewed as being simply a "bent pipe" which retransmits the uplinked information streams along a downlink path by way of downlink beam 25. The uplink and downlink operating frequencies often differ, for reasons related to the gain of

35

user receiving antennas relative to those of a ground station, and possibly also because of the relative efficiencies of electronic components at the different uplink and downlink frequencies.

5 **[0004]** Ideally, spacecraft 20 would include a "transponder" which would receive all the uplinked signals, amplify them, and retransmit the amplified signal along downlink beam 25 to the users. However, because of limitations on the undistorted power available from available transponders, 10 many transponders are used, each operating at a somewhat different frequency within the available uplink/downlink frequency band. In one current application, the spacecraft includes thirty-two transponders or physical channels, each of which handles multiple separate programs. A program may 15 include several primary streams of data, such as audio and video and security data.

[0005] In the abovementioned current application, the signal streams are in digital form, and the primary program streams are time-division multiplexed (TDM) within the channel 20 defined by the transponder. Those skilled in the art know that such time division multiplexing requires advanced controls for assigning the information packets of the various independent signal channels to the signal path without overlap of the packets. The downlink signals arriving at the user terminals 25 1, 2, . . . , N of FIGURE 1 by way of antenna beam 25 are so encoded. In addition, the information content sent over the satellite communication system may be "scrambled" or encoded in some additional way, not related to the mode of delivery over the spacecraft, to thereby prevent use of the content by 30 persons not entitled to the content by virtue of having paid for access. In this manner, an appropriately programmed smartcard or security module is needed in order to receive the downlinked information. For example, all subscribers to the satellite system may have access to certain channels, and for 35 this purpose they require at least the slot encoding

information. While access to the encoding information may make it possible for a user to correctly receive the transmitted information on a premium channel, that transmitted information may be subject to an additional layer of encoding for which the non-paying subscriber does not have the key. Thus, a multiple-tier system is provided.

[0006] The operator of the satellite information video (and associated audio) delivery system controls the use of the delivered information stream by the use of Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM). Entitlement Control Messages allow conditional access to the keys for decrypting the video stream of interest, and are delivered to the user as an integrated part of the video program, which is to say within the same physical channel as the program content. In the case of ordinary broadcast video, the physical channel is 6 MHz "wide." In the case of a cable television system, the Entitlement Control Message may be delivered on a separate, dedicated "out-of-band" channel requiring a separate or secondary tuner. This may be done so that a user can receive security information while simultaneously viewing a traditional analog television signal in which there is no mechanism for the transmission of security information.

[0007] Typically, ECMs contain the keys necessary to descramble the program in addition to a description of the tier of subscription required to access the program. The ECMs are delivered as an MPEG transport packet, possibly every 10 milliseconds, and change periodically, possibly every 30 seconds. The ECMs are identified by the program ID number (PID) of the packet. This information is typically available through the system program guide or program map information. As a user tunes a desired channel, the receiver queries the guide information to find the PID associated with the ECM to gain access to the audio/visual streams. The receiver then finds the ECM packets related to the desired programming and

passes these packets to a smart card or security module for processing. The security module opens the packets and compares the access rights of the program with the subscription level of the receiver. If the subscription level of the receiver is sufficient to permit viewing of the program, the security module decodes the decryption key and makes it available for descrambling of the program content. For those programs which exceed the current subscription level of the receiver, those keys are not made available and the receiver will not be able to descramble the content.

[0008] Entitlement Management Messages (EMM) are encrypted packets that allow for managing the rights of the receiving users to receive or not receive program content or data. EMMs are ordinarily sent to the user with a lower priority or lesser urgency than the Entitlement Control Messages (ECMs). The EMMs can be delivered in the same physical channel or in other physical channels, so long as the receiver knows a priori where and when to find them. In receivers with limited tuners, EMMs are typically transmitted simultaneously on all the physical channels to ensure that the receiver can always receive the EMM information regardless of the channel to which the receiver is currently tuned. EMMs are delivered as part of an MPEG transport stream and identified with a specific PID in a manner similar to that of the ECMs. An electronic address that can be associated with one or more receivers is typically found within the EMM packet. Typically, the receiver will look at all ECM packets delivered by the network and compare the receiver electronic address with the electronic address delivered in the EMM. If the addresses match, the EMM message is intended for the receiver, and the receiver will act in accordance with the information delivered by the EMM.

[0009] FIGURE 2a is a simplified block diagram of processing which is performed at the head end or a ground station of a system for transmitting audio/video material to

subscribers by way of a satellite. In FIGURE 2a, a set 250 including a plurality of signal processors 251, 252, . . . , 250N each receives one of a plurality of input signal streams. In one embodiment, eight channels of audio-video (AV)

5 information are applied to each processor of set 250. Each processor processes its own set of input AV information, and produces MPEG-encoded, time-division multiplexed, channelized radio-frequency information at its output terminal, for application by way of a combining (comb) arrangement

10 illustrated as 260 to antenna 14 of FIGURE 1.

[0010] FIGURE 2b is a simplified block diagram of the processing 252 which is performed for one physical channel of FIGURE 2a. It should be understood that a channel in the arrangement of FIGURE 2b corresponds to a spacecraft

15 transponder channel, because of the need to limit the number of signals traversing each spacecraft transponder channel. For definiteness, FIGURE 2b represents physical channel 252 of FIGURE 2a. In FIGURE 2b, a plurality of audio/video sources or signal streams, which in one embodiment includes eight AV

20 streams, are applied to the system. The eight audio/video streams of FIGURE 2b are designated "transponder channel II," thereby representing by a roman numeral that these signals are related to the "second" spacecraft transponder channel. The eight AV streams are applied over a plurality of signal paths

25 210a, 210b, . . . , 210N to a corresponding plurality of MPEG encoders 212a, 212b, . . . , 212N. MPEG encoding is advantageous for limiting or controlling the bandwidth of each video stream. Other compression techniques could also be used. It should be understood that some content channels may contain

30 information other than video, which may require other encoding. The MPEG-encoded signals are transmitted from encoders 212a, 212b, . . . , 212N by way of paths 214a, 214b, . . . , 214N, respectively, to a transport multiplexer (MPX) 216. In

addition to the MPEG-encoded content, the MPEG-encoded

35 Transport multiplexer also receives user guide information over

a path 217 from a block 218 and dummy EMM/ECM information over a path 219 from a block 220. The dummy EMM/ECM information is merely a "place holder" in the multiplexed data stream for the actual EMM/ECM information which will be transmitted.

5 Transport multiplexer 216 combines the input information onto a single path 224. In one version of the prior art, the multiplexing is performed in a time-division-multiplex (TDM) manner, in which the information to be transmitted is broken into "packets," which are then interleaved in time. The
10 multiplexed information from multiplexer 216 is applied over a path 224 to an encryption apparatus illustrated as a block 230. Encryption block 230 encrypts the multiplexed data stream using a key provided over a path 233 by a key generator 232.

[0011] Encryption apparatus 230 of FIGURE 2b also
15 substitutes the key and access information into the space occupied in the incoming data stream by the dummy EMM/ECM bits. This step is illustrated in FIGURE 2c, in which the stream of dummy ECM information currently traversing the encryptor is illustrated as 290. In FIGURE 2c, the ECM information is
20 inserted into the blank or dummy ECM. The ECM information contains the keys associated with a single program and information regarding the purchase rights necessary for a receiver to gain access to the keys. This ECM packet may be further encrypted with a high level system key to limit access.
25 In FIGURE 2c, the entire content K1 is illustrated as being decomposed into smaller sub-units K1a, K1b, K1c, . . . , K1X, representing all the information and keys associated with program 1. The resulting stream of encrypted TDM-multiplexed information produced by encryption block 230 of FIGURE 2b, with
30 its EMM/ECM information, is sent over a path 239 to a conventional transmitter, illustrated as a Modulator and Power Amp block 240. Transmitter block 240 modulates the signal onto one or more carriers, and raises the power of the signal. The resulting modulated, high power signal is sent from transmitter
35 block 240 of FIGURE 2b to combiner 260 of FIGURE 2a for

combination with other streams of modulated, high power signals and for application of the combined signals to antenna 14 of FIGURE 1 for transmission to the spacecraft 20. The carrier frequency (frequencies) onto which the signals are modulated by each processor of set 250 of FIGURE 2a is often selected in conjunction with the capabilities of the spacecraft to aid in separation of the modulated carriers into the available transponder channels of the spacecraft.

[0012] At the spacecraft 20 of FIGURE 1, the uplinked groupings of channels are frequency-converted and amplified for retransmission to Earth. FIGURE 3 is a simplified block diagram of the processing at the spacecraft. In FIGURE 3, receiving or uplink antenna 22 receives the uplinked encoded TDM signals and couples the signals to a frequency separation filter 310, which routes the signals, according to their frequencies, by way of a plurality of signal paths designated 312a, 312b, . . . , 312N to a like plurality of transponders 301, 302, . . . , 300N. Each transponder illustrated in FIGURE 3 includes a low-noise amplifier (LNA) for amplifying the received signals to compensate for path and other losses. It should be understood that the LNA could precede, rather than follow, the frequency separation filter 310. Each transponder 301, 302, . . . , 300N also includes a frequency converter, for converting the uplink frequency of each group of channels to a different frequency for transmission over a downlink to the users on Earth. The downlink frequencies are different among the groups of channels, for easy frequency separation. Each transponder of FIGURE 3 also includes a power amplifier, for amplifying the frequency-converted signals in the transponder channel, to aid in overcoming losses in the downlink signal path to the user. The frequency-converted, amplified signals produced at the output of each channel 301, 302, . . . , 300N are applied to a combining arrangement, which may be a frequency-sensitive combiner, for forming a combined downlink signal for application to the downlink antenna 24 of FIGURE 1.

[0013] FIGURE 4 illustrates an arrangement 426 which might be found at a user, such as at user 2 of set 26 of users of FIGURE 1. In FIGURE 4, the user 2 includes an antenna 414 directed toward the spacecraft 20 of FIGURE 1, for receiving the downlink signal, possibly including 32 transponder channels, each carrying the time-division information from eight audio/video channels together with EMM/ECM information. A receiver illustrated as a block 410 in FIGURE 4 selects for reception one of the 32 downlinked channels, and produces on a signal path illustrated as 412 the stream of corresponding data. A transport demultiplexer or demultiplexor (deMux) block 416 receives the time-division multiplexed data stream and the encryption codes. The ECM information is provided to a smartcard or security module illustrated as 417 that compares the codes with the authorizations of the local user, and if authorized, provides keys for the transport demultiplexer 416 to descramble, decompress, and process the program for viewing on a television receiver 418 according to the selected audio/visual channel.

[0014] FIGURE 7a illustrates the general tenor of the key distribution in the prior-art arrangement illustrated with reference to FIGURES 1, 2a, 2b, 2c, 3, and 4. As illustrated in FIGURE 7a, each of the encryption blocks 216a, 216b, . . . , 216N of the various processors 251, 252, . . . , 250N, respectively, of each of the physical channels, receives, over a path 233, keys produced by key generator 232. Each of the encryption blocks receives the keys for programs carried over the physical channel associated with the processor, and encodes the keys in the form of ECMs for the physical channel onto the signals traversing its own physical channel.

[0015] Non-legitimate access to the content of a system such as that set forth above in conjunction with FIGURES 1, 2a, 2b, 3, and 4 can be gained by compromising either the ECM or the EMM streams distributed to a receiver. In the case of ECM, a hacker would likely enable the viewing of a

particular program or program segment, while in the case of the EMM, the hacker would potentially generate access to all encrypted materials on the network for an indefinite period of time. The hacker needs only to access the single physical channel in which the ECM or EMM information is delivered, and store the information for analysis and information extraction. This can be accomplished in the arrangement of FIGURE 4 by the use of a computer illustrated as a block 420 connected to receive the audio/video data stream and the EMM/ECM data on signal path 412. The analysis can be done off-line once the information is stored. Once the hacker has succeeded in breaking the ECM, he can access all programming which uses the same ECM, and if the EMM can be determined, he can access all materials.

[0016] Improved or alternative information delivery systems are desired.

Summary of the Invention

[0017] A method according to an aspect of the invention is for communicating data over plural channels. The method comprises the steps of selecting data to be communicated, encryption information, and encrypting the data with the encryption information to thereby produce encrypted data. The selected data may be video information. The encryption information is broken into portions. The encrypted data is communicated by way of at least one channel of the plural channels. In one mode of the method, the encrypted data is communicated over but a single channel. At least some of the portions of the encryption key information are communicated over at least one of the plural channels other than a channel over which the encrypted data is communicated.

[0018] According to another aspect of the invention, a method for providing program information to subscribers comprises the steps of selecting a plurality of information streams to be communicated to the subscribers, and encoding

each of at least some of the information streams with individual entitlement control information to thereby generate entitlement encoded information streams. Each element of the individual entitlement control information is broken into plural portions. The encoded information streams are communicated to the subscribers, with each of the encoded information streams being communicated over one or more of a plurality of independent channels. The plural portions of the entitlement control information are communicated to the subscribers, with at least some of the portions of each entitlement control information being communicated over separate ones of the independent channels. When different subscribers have different program entitlements, the method comprises the further step of generating individual entitlement management commands identifying those information streams of a particular program to which a corresponding subscriber is entitled. Each of the individual entitlement management commands is broken into plural portions. The entitlement management commands are communicated to the subscribers over at least some of the independent channels, with at least some of the portions of each of the individual entitlement management commands being communicated over separate ones of the independent channels. At each subscriber location, the information is simultaneously decoded in at least plural ones of the independent channels to thereby form decoded information. From the decoded information, at least that one of the individual entitlement management commands applicable to the subscriber is reconstituted, to thereby form a reconstituted entitlement management command. According to a further mode of this aspect of the method of the invention, only those of the information streams, entitlement encoded information streams, and entitlement control information corresponding to the reconstituted entitlement management command are made available.

[0019] A method according to another aspect of the

invention is for providing program information to subscribers, where each subscriber has one of a plurality of different program entitlements. This method comprises the steps of selecting a plurality of information streams to be communicated to the subscribers, and encoding each of at least some of the information streams with individual entitlement control information to thereby generate entitlement encoded information streams. According to this aspect of the invention, the method breaks each element of the individual entitlement control information into plural portions. The information streams are communicated to the subscribers, with each of the information streams being communicated over one of a plurality of independent channels. The plural portions of the entitlement control information are communicated to the subscribers, with at least some of the portions of each individual entitlement control information being communicated over separate ones of the independent channels. Individual entitlement management commands are generated, identifying those information streams of a particular program to which a corresponding subscriber is entitled. Each of the individual entitlement management commands is broken into plural portions. The entitlement management commands are communicated to the subscribers over at least some of the independent channels, with at least some of the portions of each of the individual entitlement management commands being communicated over separate ones of the independent channels. At each subscriber location, the information in at least plural ones of the independent channels is simultaneously decoded to thereby form decoded information, and from the decoded information, at least that one of the individual entitlement management commands applicable to the subscriber is reconstituted, to thereby form a reconstituted entitlement management command. At each the subscriber location, only those of the information streams, entitlement encoded information streams, and entitlement control information corresponding to the reconstituted entitlement

management command is made available for display.

Brief Description of the Drawing

[0020] FIGURE 1 is a simplified block diagram of a
5 prior art satellite-based subscriber video distribution system;
FIGURE 2a is a simplified block diagram of a
plurality of processing units located at a head end or ground
station of the system of FIGURE 1, FIGURE 2b illustrates
details of one of the processing units of FIGURE 2a, and FIGURE
10 2c represents the manner in which the various keys are inserted
by the encryptor of FIGURE 2b into the locations of the dummy
EMM/ECM data in the data stream;
FIGURE 3 is a simplified block diagram of the
transponder arrangement of the spacecraft of FIGURE 1;
15 FIGURE 4 is a simplified block diagram of the
equipment that an ultimate user of the system of FIGURES 1, 2a,
2b, and 3 may have available;
FIGURE 5 is a simplified block diagram of a plurality
of processing units located at the head end or ground station
20 of the system of FIGURE 1 according to an aspect of the
invention;
FIGURE 6 is a representation of the manner in which
the key information is transmitted in a given transponder
channel; and
25 FIGURES 7a and 7b illustrate the general tenor of the
key distribution for the prior art and according to an aspect
of the invention, respectively.

Description of the Invention

30 [0021] According to an aspect of the invention, the
Entitlement Control Messages (ECM) and Entitlement Management
Messages (EMM), or at least one of them, or their equivalent,
are broken into different portions or parts, and each of the
portions or parts is transmitted to the user or subscriber
35 location by means of a separate channel of the system. In the

context of a satellite-based video distribution system (where the term "video" includes its associated audio), the ECM and/or the EMM keys are broken into plural portions or pieces, and each of the plural portions is transmitted from the spacecraft to the users on a separate one of the independent transponders of the spacecraft. In the abovementioned example, there are 32 discrete transponders over which content is transmitted, so the ECM and/or EMM keys can be broken into as many as 32 parts, with one part being distributed on each of the transponder channels. In the case of a cable television system, there is only one physical channel, which is divided into a plurality of frequency bands, each containing one part of the ECM and EMM keys. At the authorized user or subscriber location, the downlinked channels are all recovered, as, for example, by providing one conventional receiver for each transponder channel, and the key portion information is made simultaneously available to the user. The division of the keys into multiple portions is reversed, and the keys become available for use by the user.

[0022] In a particularly advantageous embodiment of the invention, the receiver, instead of being a group of conventional receivers, is instead a multi-channel signal receiver such as that described in PCT Patent application 03/08365, filed March 19, 2003 for McNeely. The McNeely application describes a receiver which enables a plurality of frequency channels to be simultaneously tuned so that broadcast channel programs included within the frequency channels may be simultaneously accessed. Signal processing circuitry including a filter bank is coupled to the signal source, and is operative to simultaneously provide baseband signals corresponding to the plurality of broadcast channel programs.

[0023] The simultaneous reception provided by the receiver of the abovementioned PCT application is accomplished, at least in part, by alias cancellation. The alias-cancelling reception provides a way to apply digital signal processing to

radio-frequency (RF) signals, with relatively low clock rates. Those skilled in the art know that the term "radio frequency," previously understood in a restricted manner, now has a meaning which embraces virtually all signal frequencies other than those in the range of visible light and ionizing radiation.

[0024] FIGURE 5 is a simplified block diagram of a system including a plurality of processing units located at the head end or ground station of the system of FIGURE 1 according to an aspect of the invention. In FIGURE 5, it is assumed that 32 transponder channels are available on the satellite (not illustrated in FIGURE 50), each capable of handling 8 audio/visual (AV) channels, together with EMM/ECM and other ancillary information. Of course, more or fewer transponder channels may be available, and each transponder channel may be capable of handling more or fewer A/V channels, and the corresponding numbers of elements in FIGURE 5 are adjusted accordingly. In the arrangement of FIGURE 5, a set of eight AV channels AV_1, AV_2, \dots, AV_8 (one spacecraft transponder's worth of signals) are applied to the inputs of a corresponding set 512₁ of eight MPEG encoders 212₁, 212₂, \dots , 212₈, which perform MPEG encoding as in the arrangement of FIGURE 2b. The MPEG-encoded AV information is coupled from encoders 212₁, 212₂, \dots , 212₈ to first transport multiplexer (MPX) 216₁ of a set 516 of transport multiplexers, which also receives guide and dummy EMM/ECM information as in the arrangement of FIGURE 2b, for time-division multiplexing the data onto a single path 224₁. The time-division multiplexed data is coupled to a first encryptor 530₁, of a set 530 of encryptors, for encryption by means of a key applied over a path 534₁. Similarly, a set of eight A/V channels $AV_9, AV_{10}, \dots, AV_{16}$ are applied to the inputs of a corresponding set 512b of eight MPEG encoders 212₉, 212₁₀, \dots , 212₁₆, which perform MPEG encoding in the same manner as encoders 212₁, 212₂, \dots , 212₈. The MPEG-encoded AV information is coupled from encoders 212₉, 212₁₀, \dots , 212₁₆ to second transport multiplexer (MPX) 216₂ of set 516, which

also receives guide and dummy EMM/ECM information, for time-division multiplexing the data onto a single path 224₂. The time-division multiplexed data is coupled to a second encryptor 530₂ of set 530 for encryption by means of a key applied over a path 534₂. Other groups of eight AV signals are similarly handled. For completeness, the last group is described, namely group of AV signals AV₂₄₈, AV₂₄₉, . . . , AV₂₅₆. In particular, a set of eight A/V channels AV₂₄₈, AV₂₄₉, . . . , AV₂₅₆ is applied to the inputs of a corresponding set of eight MPEG encoders 212₂₄₈, 212₂₄₉, . . . , 212₂₅₆ of set 512N, which perform MPEG encoding in the same manner as encoders 212₁, 212₂, . . . , 212₈. The MPEG-encoded AV information is coupled from encoders 212₂₄₈, 212₂₄₉, . . . , 212₂₅₆ to thirty-second transport multiplexer (MPX) 216₃₂ of set 516, which also receives guide and dummy EMM/ECM information, for time-division multiplexing the data onto a single path 224₃₂. The time-division multiplexed data is coupled to a thirty-second encryptor 530₃₂ of set 530 for encryption by means of a key applied over a path 534₃₂. The keys are generated by a key generator block illustrated as 532.

[0025] Encryptors 530₁, 530₂, . . . , 530₃₂ of set 530 of FIGURE 5 differ somewhat from the corresponding encryptors of FIGURE 2b. More particularly, each encryptor of set 530 of encryptors does not load the key information into the stream of data as described in conjunction with FIGURE 2c. Taking encryptor 530₁ as being representative, the key information is distributed in the manner illustrated in FIGURE 6.

[0026] In FIGURE 6, the keys which are inserted into the dummy EMM/ECM slots by encryptor 530₁ of FIGURE 5 are arranged in a manner such that at least some of the slots contain keys or key portions from other transponder channels. More particularly, the key information distribution represented in FIGURE 6 includes keys K_{1a}, K_{2a}, K_{3a}, K_{4a}, K_{5a}, . . . , K_{Na}. Key K_{1a} provides partial decoding information for program 1, corresponding to AV₁ of FIGURE 5, which program is carried on

the same transponder channel as K_{1a} . However, keys K_{2a} , K_{3a} , K_{4a} , K_{5a} , . . . , K_{Na} carry partial decryption information for programs carried on transponder channels other than the first transponder channel. That is, keys K_{2a} , K_{3a} , K_{4a} , K_{5a} , . . . , K_{Na} are related to program a on transponder channels 2, 3, 4, 5, . . . , N, respectively. The remaining portions of the program 1 key, namely K_{1b} , K_{1c} , K_{1d} , K_{1e} , . . . , K_{1n} are carried on other transponder channels. Similarly, the remaining portions of the keys for programs 2 through N are distributed among various transponder channels. Thus, the corresponding set of keys on the second transponder channel, corresponding to AV9, AV10, . . . , AV16 of FIGURE 5, could include, for example, K_{1b} , K_{2b} , K_{3b} , K_{4b} , K_{5b} , . . . , K_{Nb} , which would be the keys for decoding the second (b) program on each of the transponder channels. Other encryptors of set 530 of encryptors of FIGURE 5 carry other sets of keys. The last encryptor of FIGURE 5, namely encryptor 530_{32} , inserts encryption keys K_{1m} , K_{2m} , K_{3m} , K_{4m} , K_{5m} , . . . , K_{Nm} into its dummy EMM/ECM locations in the data stream. Thus, all the keys are transmitted, but many of them are transmitted over transponder channels other than those carrying the corresponding program. In essence, the smaller sub-units K_{1a} , K_{1b} , K_{1c} , . . . , K_{1X} of a key K_1 together constitute the information contained in K_1 ; each sub-unit might represent one byte, or a group of bytes, of the information in K_1 , and these sub-units are distributed for substantially simultaneous transmission over a plurality of channels.

[0027] In the context of a traditional spacecraft delivery system, the distribution of the keys for the various programs among the spacecraft transponders might not be acceptable, because of the inability of the single-transponder-channel receiver 410 to receive the keys for all the associated program material. According to an aspect of the invention, a multiple-transponder-channel receiver is used at the subscriber location to receive at least the number of channels required to access both a program and the associated encryption key(s). In

the simplest case, such as that described in conjunction with FIGURE 6, a two-transponder-channel receiver would be required, one for the program on a given transponder, and a second for the corresponding key, which would, in general, be on a different transponder. Thus, when it is desired to receive program a from transponder channel 3, the program is accessed through transponder channel 3, but the corresponding key K3a is retrieved from transponder channel 1 (illustrated in FIGURE 6). Thus, a multichannel receiver is required, in general, in order to access both a program and its associated key.

[0028] FIGURE 7b illustrates the general tenor of the key distribution according to an aspect of the invention. In FIGURE 7b, the processors 251, 252, . . . , 250N include their individual encryption blocks 216a, 216b, . . . , 216N, respectively, as in FIGURE 7a. A key generator and decomposer illustrated in FIGURE 7b as a block 232' generates the keys, but distributes them differently than does generator 232 of FIGURE 7a. More particularly, generator 232' produces key 1 in the form of ECM_a , key 2 in the form of ECM_b , . . . , and key_N in the form of ECM_N . In this context, $ECM_a = key_{1a}; key_{2a}; . . . , key_{Na}$, $ECM_b = key_{1b}; key_{2b}; . . . , key_{Nb}$, . . . , and $ECM_N = key_{1a}; key_{2a}; . . . , key_{Na}$.

[0029] More complex assignments of the key information are possible. For example, it is possible to degenerate a key into two or more portions, and to transmit each of the two portions on a different transponder channel. A multichannel receiver will still be able to access all of the keys for all of the programs, so long as the additional processing power is available. In general, each key could be broken into many portions, and a multichannel receiver at the subscriber end can reconstitute the appropriate key, so long as the locations of the various portions are known.

[0030] FIGURE 8a is a simplified illustration of the information stream in a traditional system such as a cable television system in which each separate "transponder" channel

is on (or "in") a different frequency range of the cable. In FIGURE 8a, three transponder channels are illustrated, namely transponder channels 1, 2, . . . , n. The letter "V" represents a video packet, the letter "A" represents an audio packet, the letter "E" represents EMM information, and the subscript refers to the particular program to which the packet relates. In transponder channel 1, the sequential flow of packets is V₁, V₁, A₁, E₁, V₁, V₁, A₁, E₁, V₁, V₁, A₁, E₁, . . . , all relating to program information 1. In essence, transponder channel 1 carries all the program 1 information, together with its EMM information. Similarly, transponder 2 carries sequential packets V₂, V₂, A₂, E₂, V₂, V₂, A₂, E₂, V₂, V₂, A₂, E₂ . . . and transponder n carries sequential packets V_n, V_n, A_n, E_n, V_n, V_n, A_n, E_n, V_n, V_n, A_n, E_n. Each transponder channel thus carries its own program material and the associated code. Since the ECM key information is often provided every few milliseconds, so that a subscriber making a new connection does not have to wait too long for appearance of a decrypted program, and since the ECM keys change every few seconds, as for example every 30 seconds, it is possible to break the ECM information in time rather than in data content. This is illustrated in FIGURE 8b, in which transponder 1 carries program information 1, transponder 2 carries program information 2, . . . , and transponder n carries program information n. In the arrangement of FIGURE 8b, by contrast with the arrangement of FIGURE 8a, the ECM information is switched among the various transponder channels. More particularly, in FIGURE 8b, transponder channel 1 carries sequential packets V₁, V₁, A₁, E₁, V₁, V₁, A₁, E₂, V₁, V₁, A₁, E_n, . . . , transponder channel 2 carries sequential packets V₂, V₂, A₂, E₂, V₂, V₂, A₂, E_n, V₂, V₂, A₂, E₁, . . . , and transponder channel n carries sequential packets V_n, V_n, A_n, E_n, V_n, V_n, A_n, E₁, V_n, V_n, A_n, E₂, Thus, in the arrangement of FIGURE 8b, the complete ECM message required to decode or decrypt the program data is broken into time

sequential portions, such as portions E1, E2, . . . , En, . . . and these time-sequential portions of the complete ECM message are switched among the various individual channels.

[0031] The multichannel receiver may be an array of
5 conventional tuned receivers, or it may be the abovementioned alias-cancelling multichannel receiver.

[0032] Those skilled in the art know that the functions of a system may be illustrated with some functions of a block incorporated into the adjacent block, without any
10 change to the essence of the invention. For example, while the decomposition of the keys has been illustrated in FIGURE 7b as being performed by a "key generator and decomposer" block 232', the keys could be generated and distributed to all the encryption blocks 216a, 216b, . . . , 216N, and the
15 decomposition could be performed in the encryption blocks. Further, the examples have illustrated transmission over a physical channel of keys arranged in a particular ordering, but the ordering of the keys need follow no particular rule. While the description has referred to breaking the keys into
20 portions, and transmitting the portions over different transponders, it is possible to transmit ECM information for a program in complete form over a transponder other than the one on which

[0033] A method according to an aspect of the
25 invention is for communicating data over plural channels (301, 302, . . . , 300N). The method comprises the steps of selecting data to be communicated (A/V information), encryption information (K_{1a} , K_{2a} , K_{3a} , . . . , K_{Na}) and encrypting the data with the encryption information to thereby produce encrypted
30 data. The selected data may be video information. The encryption information is broken into portions (ECM_a , ECM_b , . . . , ECM_N). The encrypted data is communicated by way of at least one channel (transponder channel I) of the plural channels (301, 302, . . . , 300N). In one mode of the method,
35 the encrypted data is communicated over but a single channel

(transponder channel I). At least some of the portions of the encryption key information are communicated over at least one of the plural channels (301, 302, . . . , 300N) other than a channel over which the encrypted data is communicated.

5 **[0034]** According to another aspect of the invention, a method for providing program information to subscribers (426) comprises the steps of selecting a plurality of information streams (A/V information) to be communicated to the subscribers, and encoding each of at least some of the
10 information streams with individual entitlement control information to thereby generate entitlement encoded information streams. Each element of the individual entitlement control information is broken into plural portions. The encoded information streams are communicated to the subscribers, with
15 each of the encoded information streams being communicated over one of a plurality of independent channels (301, 302, . . . , 300N), or at least over fewer than all the physical channels. The plural portions of the entitlement control information are communicated to the subscribers, with at least some of the
20 portions of each entitlement control information being communicated over separate ones of the independent channels (301, 302, . . . , 300N). When different subscribers have different program entitlements, the method comprises the further step of generating individual entitlement management
25 commands identifying those information streams of a particular program to which a corresponding subscriber is entitled. Each of the individual entitlement management commands is broken into plural portions. The entitlement management commands are communicated to the subscribers over at least some of the
30 independent channels (301, 302, . . . , 300N), with at least some of the portions of each of the individual entitlement management commands being communicated over separate ones of the independent channels (301, 302, . . . , 300N). At each subscriber location, the information is simultaneously decoded
35 in at least plural ones of the independent channels to thereby

form decoded information. From the decoded information, at least that one of the individual entitlement management commands applicable to the subscriber is reconstituted, to thereby form a reconstituted entitlement management command.

5 According to a further mode of this aspect of the method of the invention, only those of the information streams, entitlement encoded information streams, and entitlement control information corresponding to the reconstituted entitlement management command are made available.

10 **[0035]** A method according to another aspect of the invention is for providing program information to subscribers, where each subscriber has one of a plurality of different program entitlements. This method comprises the steps of selecting a plurality of information streams to be communicated
15 to the subscribers, and encoding each of at least some of the information streams with individual entitlement control information to thereby generate entitlement encoded information streams. According to this aspect of the invention, the method breaks each element of the individual entitlement control
20 information into plural portions. The information streams are communicated to the subscribers, with each of the information streams being communicated over one of a plurality of independent channels (301, 302, . . . , 300N). The plural portions of the entitlement control information are
25 communicated to the subscribers, with at least some of the portions of each individual entitlement control information being communicated over separate ones of the independent channels (301, 302, . . . , 300N). Individual entitlement management commands are generated, identifying those
30 information streams of a particular program to which a corresponding subscriber is entitled. Each of the individual entitlement management commands is broken into plural portions. The entitlement management commands are communicated to the subscribers over at least some of the independent channels
35 (301, 302, . . . , 300N), with at least some of the portions of

each of the individual entitlement management commands being communicated over separate ones of the independent channels. At each subscriber location, the information in at least plural ones of the independent channels is simultaneously decoded to thereby form decoded information, and from the decoded information, at least that one of the individual entitlement management commands applicable to the subscriber is reconstituted, to thereby form a reconstituted entitlement management command. At each the subscriber location, only those of the information streams, entitlement encoded information streams, and entitlement control information corresponding to the reconstituted entitlement management command is made available for display.